UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/187,700	11/06/1998	HIROYUKI KOBAYASHI	3408.62676	3400

24978 7590 12/02/2002

GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO, IL 60606

EXAMINER
MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/02/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/187,700	Applicant(s) KOBAYASHI ET AL.	
	Examiner Douglas J. Meislahn	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 September 2002* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 23 September 2002 that amended claims 15, 18, and 19. The JP `021 reference was apparently considered by the examiner originally examining the application, as indicated on the 1449. Nevertheless, the examiner currently handling this case also reviewed the reference.

Response to Arguments

2. Applicant's arguments filed 23 September 2002 have been fully considered but they are not persuasive. Applicant's description of support for claim 7 does not correspond to the claim. Unlike applicant's description of the claim, PW1 is NOT encrypted with PW2; instead PW1 encrypts both the random number data (as described in applicant's comments) and PW2, which contradicts applicant's description. The encrypted second password is then decrypted with PW2 and, according to the claim, results in PW1. As a formula, applicant's claim looks thus: $(D_{PW2}(E_{PW1}(PW2)))=PW1$.

3. With respect to the 101 rejection of claim 15, the subject matter of the claim is nonfunctional descriptive material, which is not patentable. See MPEP 2106 IV. B 1 (b).

4. Applicant alleges that the cited references do not show "generating different key data for each of a plurality of unit storage areas of said storage medium". This does not mandate more than of unit storage area, and as such one generated key meets the limitations of that phrase.

5. The examiner agrees that Ganesan does not disclose "encrypting each said different key data for each unit storage area with said password". However, the

limitations not met by Ganesan, predominantly the password, are rendered obvious by Kaufman.

6. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

7. In response to applicant's argument that "the purposes and benefits of the cited references are different from the present invention", the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

8. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, computational efficiency, achieved by encrypting with a symmetric algorithm, would lead one of ordinary skill in the art to combine the teachings of Kaufman with Ganesan.

9. In response to applicant's argument that Ganesan is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, encrypting a key with a public key is relevant to encrypting a key with a symmetric key.

10. Applicant argues that Kaufman's focus is to avoid encrypting information. This ignores Kaufman's explicit teaching, cited previously by the examiner, of a password key being used to encrypt a file key. As such, applicant's characterization of Kaufman as teaching away from the use of key data is not persuasive.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

12. Claim 7 is rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 7 dictates that the first password encrypts not only the encryption key, but also a second password. The

encrypted second password is decrypted by the second password, which results in the first password. How exactly does this work, and where is it supported?

Claim Rejections - 35 USC § 101

13. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 15 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The data on the storage medium in claim 15 do not cause a computer to act in a specific fashion, and as such do not compose a data structure.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 1, 6-8, and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan (5748735) in view of Kaufman (6178508).

Ganesan's fourth figure shows a symmetric key being generated in element 330. Subsequently, this key is encrypted. In element 390, the encrypted symmetric key and data encrypted with that symmetric key are stored. With the exception of the password stipulation, clause one is hereby rendered obvious. Clause two is anticipated by elements 390 and 380. Step 580 in figure 5 shows reading the encrypted symmetric

key from a storage medium, meeting the limitations of the third clause. The next step, element 585, anticipates the non-password portion of clause four. Element 590 anticipates clause five.

In lines 27-31 of column 6, Ganesan stipulates that the encrypted file and encrypted key are stored on an associated memory device. This reads on generating a key for a storage area. As is apparent from the abstract, the intent of Ganesan is to provide storage for a multitude of files. The writing of the encrypted key to the memory device has already been described.

Ganesan says that the symmetric key is encrypted with a private key, not a password, although there are some functional similarities between the two: both should be known only by the holder, and both are often used for authentication. There are also several differences, such as the former being used in a public key cryptosystem and the latter, when acting as a key, being used in a symmetric key cryptosystem, as shown by Kaufman in lines 14-24 of column 6. Another difference is that passwords can generally be easily remembered while private keys practically require storage on a computer readable medium. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a password as taught by Kaufman to encrypt the symmetric key in Ganesan. As is evident from Kaufman's exclusive-OR operation, this would conserve processing power.

Claim 6 is covered by Kaufman's plurality of passwords and quorum needed to decrypt. See columns five and six. Repeated encryptions of a secret are well-known and thus claim 7 is anticipated.

16. Claims 2 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Kaufman as applied to claim 1 above, and further in view of Cruts et al. (4780905).

Ganesan and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not say that the key is generated per the logic sector of the storage medium. In lines 46-48 of column 2, Cruts et al. say that a decryption key is based on a formula that uses the disc address of data. In lines 24 and 25 above, they say that this saves the user from needing to know and remember the encryption key. This is not to say that the encryption key is deleted (see abstract). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to associate the keys in Ganesan with the memory device on which they were to be stored by forming them according to an algorithm based on the address of the data, thereby saving the user from needing to remember the encryption keys.

17. Claims 3, 4, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Kaufman as applied to claim 1 above, and further in view of Schneier (*Applied Cryptography*).

Ganesan and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not say that new symmetric keys are generated each time data is written to a spot in the

memory device. On pages 6 and7, Schneier mentions the ciphertext-only attack, which relies on knowledge of multiple ciphertexts encrypted with the same encryption key. One obvious response to this is to use keys but once, which, depending on the algorithm, can verge on a one-time pad, which is a perfectly secret algorithm. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to generate new keys, as suggested by Schneier, every time data is written to a memory device in Ganesan.

Neither Kaufman nor Ganesan say that the symmetric key is made by combining a predetermined number of pieces of random data. On page 173, Schneier says that good keys are random-bit strings generated by an automatic process. One way to achieve this is to generate the key from a reliably random source. This source reads on applicant's predetermined number of pieces of random data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to generate the symmetric key in Kaufman using random pieces of data as taught by Schneier in order to have a "good" key.

18. Claim 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Kaufman as applied to claim 1 above, and further in view of Blakley, III et al. (5677952).

Ganesan and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not present a system by which passwords are changed. In lines 6-25 of column 7, Blakley,

III et al. show a method of changing a password that consists of decrypting data with the old password and re-encrypting it with the new password. In Blakley, III et al., these two steps occur simultaneously. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to change passwords in the system of Ganesan and Kaufman according to the method of Blakley, III et al., thereby letting users update their passwords.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
November 26, 2002

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100